

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
DANVILLE DIVISION

IN THE MATTER OF THE SEARCH OF Red
in color Apple iPhone IMEI no.
357348095928018 contained in a red
protective case.

Case No. 4:23mj5

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR RULE 41 SEARCH
WARRANT**

I, Richard Wright, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device, described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7) and am empowered by law to conduct investigations of, and to make arrests for, offenses in violation of Title 18 and Title 21 of the United States Code.

3. Specifically, I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) and have been so employed since September 2019. I am currently assigned to the Richmond Division of the FBI, Charlottesville Resident Agency. In addition to my employment as an FBI TFO, I serve as a Police Officer for the Danville Police Department and have been so employed since August 2012. I am presently and have been previously assigned to investigate a variety of criminal matters, to include violent criminal acts, gangs, and firearm investigations. Further, I have experience and training in a variety of investigative and legal

matters, including the topics of lawful arrests, the drafting of search warrant affidavits, and probable cause. I have participated in numerous criminal investigations focused on firearms, armed drug trafficking violations, and criminal street gangs. I have investigated violations of Title 18, United States Code, Section 1962 (Racketeering Influenced Corrupt Organizations Act); Title 18, United States Code, Section 1959 (Violent Crimes in Aid of Racketeering); Title 18, United States Code, Sections 922 *et seq.* (Firearms Offenses); and Title 21, United States Code, Sections 841 *et seq.* (Drug Offenses). I have experience in the investigation, apprehension, and prosecution of individuals involved in firearms offenses and narcotics trafficking offenses. I have also been trained on the use of cellular and electronic devices, to include performing forensic examinations on such devices.

4. The facts in this affidavit come from my personal observations, my training and experience, as well as information obtained from other law enforcement officers and in interviews with witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 922(g)(1) (Felon in Possession of a Firearm) and Title 18, United States Code, § 924(c) (Use of Firearm in Furtherance of a Crime of Violence) have been committed.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Red in color Apple iPhone IMEI no. 357348095928018 contained in a red protective case, hereinafter “Device 1.” Device 1 is currently located in at the Danville, Virginia Police Department in Danville, Virginia. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about March 10, 2022, law enforcement began to investigate Maurice Demetrius METTS, aka “Spazz,” and his involvement as a leader in the Bloods, a nationally known gang founded in Los Angeles in the 1970s as a response to the rise and dominance of the Crips street gang.

7. During this investigation, law enforcement obtained state search warrants concerning the Facebook accounts operated by several members of the Bloods. Pursuant to the search warrants, law enforcement reviewed the account records and witnessed messages from the Facebook account “Jonathan Jaxkson” (USER ID: 100045461596661), an account known to be operated by METTS.

8. On or about July 22, 2022, law enforcement executed a state search warrant for the Facebook account, and later received the requested records. Law enforcement reviewed the provided records and witnessed the following:

- a. Multiple user attributes consistent with the account being operated by METTS such as multiple photographs of METTS, the account answering to METTS’ legal names as well as his known alias, the date of birth provided for the account matching METTS’, and the account providing its email as mauricemetts116@gmail.com.
- b. The account arranged meetings and talked about criminal acts completed by subordinate members of the Bloods.

9. On or about August 25, 2022, law enforcement executed an additional state search warrant concerning the email account “mauricemetts116@gmail.com.” On September 4, 2022, law enforcement received the records for the account and reviewed them. Law enforcement witnessed where the email account received and forwarded multiple emails

containing Bloods documents.

10. On October 6, 2022, law enforcement executed a state search warrant at 636-1 Cardinal Village Place, Danville, Virginia. That search warrant related to METTS being a fugitive from justice for a felony probation violation as well authorizing a search for evidence of METTS possessing a firearm after being a six-time convicted felon. Upon execution of the search warrant, METTS was located as the sole occupant of the residence hiding underneath a bed, with Device 1 in his hand.

11. Pursuant to the search warrant, law enforcement conducted a search of the residence and located a Glock firearm, ammunition, and an extended magazine in a nightstand beside the bed METTS was hiding under. Law enforcement also observed in plain sight suspected controlled substances, digital scales, and packaging material indicative of distribution in the same room where METTS was apprehended along with multiple identifying documents for METTS. Indeed, some of this evidence was found on the nightstand that was storing the firearm. Therefore, the firearm was in an environment surrounded by indicia of drug distribution.

12. Shortly thereafter, on October 6, 2022, a second state search warrant for the residence was obtained concerning the distribution of controlled substances. The aforementioned items and Device 1 were seized.

13. On or about October 13, 2022, law enforcement completed a review of Device 1 pursuant to a state search warrant. During the review, law enforcement witnessed the following:

- a. Multiple user attributes consistent with Device 1 being operated by METTS. These attributes consisted of METTS answering and using his legal name as well as

known alias, METTS providing banking information, multiple photographs and videos of METTS, and the device being logged into multiple user accounts for METTS.

- b. METTS utilized Device 1 to facilitate the distribution of multiple controlled substances to multiple subjects. These transactions took place up until the morning that law enforcement executed the search warrant at 636-1 Cardinal Place Danville, VA.
- c. Multiple photographs of METTS possessing a firearm consistent with the firearm seized from 636-1 Cardinal Place, Danville, VA. On or about October 4, 2022, Device 1 conducted multiple searches through the web browser for drum style magazines that specifically fit a Glock model 22.

14. Through my training and experience in investigating firearm violations, I know the following:

- a. Suspects commonly use cellular phones and other communication devices to communicate with others about the firearms they currently possess and the location of the firearms.
- b. Suspects commonly use cellular phones and other communication devices to facilitate the selling, purchasing, trading, loaning, or stealing firearms.
- c. Suspects commonly use cellular phones and other communication devices to access web browsers, where they can conduct a search for firearm parts, ammunition, and repair/maintenance for firearms.

d. Suspects also use their cellphones to store and share media, such as videos or digital photos, showing them possessing firearms and/or accessories for firearms.

15. Moreover, cellphones generally contain data regarding criminal activity generally. For example, as detailed below, cellphones can contain GPS information, which can help law enforcement identify and locate additional co-conspirators.

16. Therefore, I believe that contents of Device 1 may contain evidence indicating violations of Title 18, United States Code, Section 922(g)(1) (Felon in Possession of a Firearm) and Title 18, United States Code, § 924(c) (Use of Firearm in Furtherance of a Crime of Violence).

TECHINCAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still

photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of

electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for

entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that the Device has

capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery”

file.

- b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

21. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection to determine whether it is evidence described by the warrant.

MANNER OF EXECUTION

23. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion

onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,


FBI Task Force Officer R. P. Wright
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on
March 9, 2023



ROBERT S. BALLOU
UNITED STATES MAGISTRATE JUDGE